El lado oscuro
Por Sebastián Vallejo

Todos los gobiernos, en grados diferentes, tienen ese oxímoron llamado unidades de inteligencia. Son, por naturaleza, oficinas siniestras. Son necesarias, se puede argumentar. Hay información que no se puede revelar en rueda de prensa. Entiendo cuál es la necesidad de interceptar comunicaciones y hacerlo de manera secreta. Me pone intranquilo que exista una agencia con esa capacidad, más aún si actúa bajo la doctrina de la Guerra Fría y la seguridad nacional. Pero entiendo su necesidad. Sin embargo, hay una delgada línea legal, y un claro abismo ético, entre usar herramientas de espionaje para atrapar delincuentes, y usarlas para acosar a ciudadanos. Parecería que la SENAIN está dando trotes al otro lado.

Hace un par de semanas, hackers subieron a la web 400gb de información sobre la empresa de ciber-espionaje Hacking Team. En su lista de clientes, todas instituciones gubernamentales, están países que recorren el amplio espectro entre dictadura y democracia: desde Sudán hasta Suiza. También consta la SENAIN. El récord de Hacking Team no es el mejor, comenzando por el hecho de vender este tipo de herramientas a países sancionados por la ONU (y negar que lo hace). El tipo de herramientas, *exploits*, utilizados para vulnerar sistemas, y otras para acceso remoto de equipos, las tenían bajo seguridad bastante laxa (ergo, la ironía de ser hackeados). Las herramientas son de ataque, y su naturaleza vuelve sospechoso su uso, especialmente cuando son utilizadas sin la debida fiscalización y autorización judicial. Chile está aclarando esto último. En Chipre ya renunció el Jefe del Departamento de Inteligencia.

La SENAIN, por su parte, mandó un comunicado negando todo y finalizando con el comodín jurídico de cómo se reservan "el derecho legal de actuar en defensa de la seguridad nacional y del prestigio del gobierno ecuatoriano", que es un paraguas para todo sin decir nada. Negar su relación contractual con Hacking Team es un formalismo legal: los documentos demostrarían que estaban trabajando a través de un intermediario [2] [3].

Pero esto se vuelve casi insignificante ante lo que indican los correos sobre Hacking Team revelados por WikiLeaks. No solo se puede leer la comunicación directa entre el personal de Hacking Team y agentes de la SENAIN. Los correos también muestran cómo, desde la SENAIN, se solicita archivos para poder manejar remotamente a usuarios cuando abren ciertos archivos u otros para "saturar" paginas y que estas se bloqueen, sugiriendo que los objetivos eran personas criticas al gobierno. La direcciones son de medios como *El Universo*, *Hoy*, *La República*, e incluyen noticias sobre las manifestaciones y asambleístas de la oposición. Los archivos para infectar equipos y manejarlos remotamente tienen nombres como: CarlosVerA.zip, preguntasyasuni.rar, Chevronasksjudge.rar. Entre lo que parecen ser los registros de sistemas infectados, hay carpetas con nombres como: Jueces, CONAIE y CNE. Hay incluso un correo donde el presunto objetivo es la página de la Federación Médica Ecuatoriana.

La SENAIN debe explicar ante los órganos que determina la Ley (la respectiva comisión de la Asamblea) sobre el uso de estas herramientas y las relaciones con la empresa cuestionada o sus intermediarios. Y debe, más que nada, aclarar a la ciudadanía este posible abuso de autoridad, violación de la privacidad y atropello a los derechos humanos.

(Actualizado) Julio 20, 2015